

# **2022 IEEE Symposium on Security and Privacy (SP 2022)**

**San Francisco, California, USA  
23-26 May 2022**

**Pages 1-649**



**IEEE Catalog Number: CFP22020-POD  
ISBN: 978-1-6654-1317-6**

**Copyright © 2022 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP22020-POD
ISBN (Print-On-Demand):	978-1-6654-1317-6
ISBN (Online):	978-1-6654-1316-9
ISSN:	1081-6011

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2022 IEEE Symposium on Security and Privacy (SP) SP 2022

## Table of Contents

Message from the Program Chairs .....	xxv
Organizing Committee .....	xxvii

### Session 1A: Fuzzing I

PATA: Fuzzing with Path Aware Taint Analysis .....	1
<i>Jie Liang (Tsinghua University, China), Mingzhe Wang (Tsinghua University, China), Chijin Zhou (Tsinghua University, China), Zhiyong Wu (Tsinghua University, China), Yu Jiang (Tsinghua University, China), Jianzhong Liu (Tsinghua University, China), Zhe Liu (Nanjing University of Aeronautics and Astronautics, China), and Jianguang Sun (Tsinghua University, China)</i>	
JIGSAW: Efficient and Scalable Path Constraints Fuzzing .....	18
<i>Ju Chen (University of California, Riverside), Jinghan Wang (University of California, Riverside), Chengyu Song (University of California, Riverside), and Heng Yin (University of California, Riverside)</i>	
BEACON : Directed Grey-Box Fuzzing with Provable Path Pruning .....	36
<i>Heqing Huang (The Hong Kong University of Science and Technology), Yiyuan Guo (The Hong Kong University of Science and Technology), Qingkai Shi (The Hong Kong University of Science and Technology), Peisen Yao (The Hong Kong University of Science and Technology), Rongxin Wu (Xiamen University), and Charles Zhang (The Hong Kong University of Science and Technology)</i>	

### Session 1B: Formal Analysis I

Automated Attack Synthesis by Extracting Finite State Machines from Protocol Specification Documents .....	51
<i>Maria Leonor Pacheco (Purdue University), Max von Hippel (Northeastern University), Ben Weintraub (Northeastern University), Dan Goldwasser (Purdue University), and Cristina Nita-Rotaru (Northeastern University)</i>	
ProVerif with Lemmas, Induction, Fast Subsumption, and Much More .....	69
<i>Bruno Blanchet (Inria Paris), Vincent Cheval (Inria Paris), and Véronique Cortier (Université de Lorraine, CNRS, Inria)</i>	

Four Attacks and a Proof for Telegram .....	87
<i>Martin R. Albrecht (Royal Holloway, University of London, United Kingdom), Lenka Mareková (Royal Holloway, University of London, United Kingdom), Kenneth G. Paterson (ETH Zurich, Switzerland), and Igor Stepanovs (ETH Zurich, Switzerland)</i>	

## Session 1C: Verification for Security

Noise*: A Library of Verified High-Performance Secure Channel Protocol Implementations .....	107
<i>Son Ho (INRIA Paris), Jonathan Protzenko (Microsoft Research), Abhishek Bichhawat (IIT Gandhinagar), and Karthikeyan Bhargavan (INRIA Paris)</i>	
A Logic and an Interactive Prover for the Computational Post-Quantum Security of Protocols..	125
<i>Cas Cremers (CISPA Helmholtz Center for Information Security, Germany), Caroline Fontaine (Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles, 91190, Gif-sur-Yvette, France), and Charlie Jacomme (CISPA Helmholtz Center for Information Security, Germany)</i>	
IronMask: Versatile Verification of Masking Security .....	142
<i>Sonia Belaïd (CryptoExperts, France), Darius Mercadier (CryptoExperts, France), Matthieu Rivain (CryptoExperts, France), and Abdul Rahman Taleb (CryptoExperts, France and Sorbonne Université, CNRS, LIP6, France)</i>	

## Session 2A: Blockchain Security I

SAILFISH: Vetting Smart Contract State-Inconsistency Bugs in Seconds .....	161
<i>Priyanka Bose (University of California, Santa Barbara, USA), Dipanjan Das (University of California, Santa Barbara, USA), Yanju Chen (University of California, Santa Barbara, USA), Yu Feng (University of California, Santa Barbara, USA), Cristopher Kruegel (University of California, Santa Barbara, USA), and Giovanni Vigna (University of California, Santa Barbara, USA)</i>	
ZeeStar: Private Smart Contracts by Homomorphic Encryption and Zero-knowledge Proofs ....	179
<i>Samuel Steffen (ETH Zurich, Switzerland), Benjamin Bichsel (ETH Zurich, Switzerland), Roger Baumgartner (ETH Zurich, Switzerland), and Martin Vechev (ETH Zurich, Switzerland)</i>	
Quantifying Blockchain Extractable Value: How dark is the forest? .....	198
<i>Kaihua Qin (Imperial College London), Liyi Zhou (Imperial College London), and Arthur Gervais (Imperial College London)</i>	

## Session 2B: Formal Analysis II

A Formal Security Analysis of the W3C Web Payment APIs: Attacks and Verification .....	215
<i>Quoc Huy Do (University of Stuttgart, Germany), Pedram Hosseyni (University of Stuttgart, Germany), Ralf Küsters (University of Stuttgart, Germany), Guido Schmitz (University of Stuttgart, Germany and Royal Holloway, University of London, UK), Nils Wenzler (University of Stuttgart, Germany), and Tim Würtele (University of Stuttgart, Germany)</i>	
Cats vs. Spectre: An Axiomatic Approach to Modeling Speculative Execution Attacks .....	235
<i>Hernán Ponce de León (Research Institute CODE - Bundeswehr University Munich) and Johannes Kinder (Research Institute CODE - Bundeswehr University Munich)</i>	
TASHAROK: Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems .....	249
<i>Mustafa Abdallah (Purdue University, United States), Daniel Woods (University of Innsbruck, Austria), Parinaz Naghizadeh (Ohio State University, United States), Issa Khalil (Qatar Computing Research Institute (QCRI), HBKU, Qatar), Timothy Cason (Purdue University, United States), Shreyas Sundaram (Purdue University, United States), and Saurabh Bagchi (Purdue University, United States)</i>	

## Session 2C: Smart Homes and Virtual Reality

SoK: Authentication in Augmented and Virtual Reality .....	267
<i>Sophie Stephenson (University of Wisconsin--Madison), Bijeeta Pal (Cornell University), Stephen Fan (University of Wisconsin--Madison), Earlene Fernandes (University of Wisconsin--Madison), Yuhang Zhao (University of Wisconsin--Madison), and Rahul Chatterjee (University of Wisconsin--Madison)</i>	
Delay Wreaks Havoc on Your Smart Home: Delay-based Automation Interference Attacks .....	285
<i>Haotian Chi (Temple University), Chenglong Fu (Temple University), Qiang Zeng (University of South Carolina), and Xiaojiang Du (Stevens Institute of Technology)</i>	
Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes .....	303
<i>Haojian Jin (Carnegie Mellon University), Gram Liu (Carnegie Mellon University), David Hwang (Carnegie Mellon University), Swarun Kumar (Carnegie Mellon University), Yuvraj Agarwal (Carnegie Mellon University), and Jason Hong (Carnegie Mellon University)</i>	

## Session 3A: Trusted Execution Environments

vSGX: Virtualizing SGX Enclaves on AMD SEV .....	321
<i>Shixuan Zhao (The Ohio State University, United States), Mengyuan Li (The Ohio State University, United States), Yinqian Zhang (Southern University of Science and Technology, China), and Zhiqiang Lin (The Ohio State University, United States)</i>	

A Systematic Look at Ciphertext Side Channels on AMD SEV-SNP .....	337
<i>Mengyuan Li (The Ohio State University), Luca Wilke (University of Lübeck), Jan Wichelmann (University of Lübeck), Thomas Eisenbarth (University of Lübeck), Radu Teodorescu (The Ohio State University), and Yinqian Zhang (Southern University of Science and Technology)</i>	
RT-TEE: Real-time System Availability for Cyber-physical Systems using ARM TrustZone .....	352
<i>Jinwen Wang (Washington University in St. Louis), Ao Li (Washington University in St. Louis), Haoran Li (Washington University in St. Louis), Chenyang Lu (Washington University in St. Louis), and Ning Zhang (Washington University in St. Louis)</i>	
A Secret-Free Hypervisor: Rethinking Isolation in the Age of Speculative Vulnerabilities .....	370
<i>Hongyan Xia (Microsoft), David Zhang (Microsoft), Wei Liu (Microsoft), Istvan Haller (Microsoft), Bruce Sherwin (Microsoft), and David Chisnall (Microsoft)</i>	
SMILE: Secure Memory Introspection for Live Enclave .....	386
<i>Lei Zhou (Southern University of Science and Technology, China), Xuhua Ding (Singapore Management University, Singapore), and Fengwei Zhang (Southern University of Science and Technology, China)</i>	

## Session 3B: Differential Privacy

Statistical Quantification of Differential Privacy: A Local Approach .....	402
<i>Önder Askin (Ruhr-University Bochum, Germany), Tim Kutta (Ruhr-University Bochum, Germany), and Holger Dette (Ruhr-University Bochum, Germany)</i>	
Locally Differentially Private Sparse Vector Aggregation .....	422
<i>Mingxun Zhou (Carnegie Mellon University, United States), Tianhao Wang (University of Virginia, United States), T-H. Hubert Chan (The University of Hong Kong, Hong Kong SAR, China), Giulia Fanti (Carnegie Mellon University, United States), and Elaine Shi (Carnegie Mellon University, United States)</i>	
Differentially Private Histograms in the Shuffle Model from Fake Users .....	440
<i>Albert Cheu (Georgetown University) and Maxim Zhilyaev (Meta Privacy)</i>	
Differential Privacy and Swapping: Examining De-Identification's Impact on Minority Representation and Privacy Preservation in the U.S. Census .....	457
<i>Miranda Christ (Columbia University), Sarah Radway (Tufts University), and Steven M. Bellovin (Columbia University)</i>	
Are We There Yet? Timing and Floating-Point Attacks on Differential Privacy Systems .....	473
<i>Jiankai Jin (The University of Melbourne), Eleanor McMurtry (ETH Zurich), Benjamin Rubinstein (The University of Melbourne), and Olga Ohrimenko (The University of Melbourne)</i>	

## Session 3C: Attack Investigations

SHADEWATCHER: Recommendation-guided Cyber Threat Analysis using System Audit Records ....	489
<i>Jun Zeng (National University of Singapore), Xiang Wang (University of Science and Technology of China), Jiahao Liu (National University of Singapore), Yinfang Chen (University of Illinois Urbana-Champaign), Zhenkai Liang (National University of Singapore), Tat-Seng Chua (National University of Singapore), and Zheng Leong Chua (Independent Researcher)</i>	
SIRAJ: A Unified Framework for Aggregation of Malicious Entity Detectors .....	507
<i>Saravanan Thirumuruganatha (Qatar Computing Research Institute), Mohamed Nabeel (Qatar Computing Research Institute), Euijin Choo (Qatar Computing Research Institute), Issa Khalil (Qatar Computing Research Institute), and Ting Yu (Qatar Computing Research Institute)</i>	
DeepCASE: Semi-Supervised Contextual Analysis of Security Events .....	522
<i>Thijs van Ede (University of Twente), Hojjat Aghakhani (University of California, Santa Barbara), Noah Spahn (University of California, Santa Barbara), Riccardo Bortolameotti (ReaQta), Marco Cova (VMware, Inc.), Andrea Continella (University of Twente), Maarten van Steen (University of Twente), Andreas Peter (University of Twente), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)</i>	
DEPCOMM: Graph Summarization on System Audit Logs for Attack Investigation .....	540
<i>Zhiqiang Xu (Chinese Academy of Sciences, China), Pengcheng Fang (Case Western Reserve University, USA), Changlin Liu (Case Western Reserve University, USA), Xusheng Xiao (Case Western Reserve University, USA), Yu Wen (Chinese Academy of Sciences, China), and Dan Meng (Chinese Academy of Sciences, China)</i>	
Measuring and Mitigating the Risk of IP Reuse on Public Clouds .....	558
<i>Eric Pauley (The Pennsylvania State University), Ryan Sheatsley (The Pennsylvania State University), Blaine Hoak (The Pennsylvania State University), Quinn Burke (The Pennsylvania State University), Yohan Beugin (The Pennsylvania State University), and Patrick McDaniel (The Pennsylvania State University)</i>	

## Session 4C: Crypto Implementations

SecFloat: Accurate Floating-Point meets Secure 2-Party Computation .....	576
<i>Deevashwer Rathee (UC Berkeley, USA), Anwesh Bhattacharya (Microsoft Research, India), Rahul Sharma (Microsoft Research, India), Divya Gupta (Microsoft Research, India), Nishanth Chandran (Microsoft Research, India), and Aseem Rastogi (Microsoft Research, India)</i>	
Multi-server Verifiable Computation of Low-Degree Polynomials .....	596
<i>Liang Feng Zhang (ShanghaiTech University) and Huaxiong Wang (Nanyang Technological University)</i>	

Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques .....	614
<i>Amit Seal Ami (William &amp; Mary), Nathan Cooper (William &amp; Mary), Kaushal Kafle (William &amp; Mary), Kevin Moran (George Mason University), Denys Poshyvanyk (William &amp; Mary), and Adwait Nadkarni (William &amp; Mary)</i>	
“They’re not that hard to mitigate”: What Cryptographic Library Developers Think About Timing Attacks .....	632
<i>Jan Jancar (Masaryk University, Brno, Czech Republic), Marcel Fourné (MPI-SP, Bochum, Germany), Daniel De Almeida Braga (Rennes University, CNRS, IRISA, Rennes, France), Mohamed Sabt (Rennes University, CNRS, IRISA, Rennes, France), Peter Schwabe (MPI-SP, Bochum, Germany, and Radboud University, Nijmegen, The Netherlands), Gilles Barthe (MPI-SP, Bochum, Germany, and IMDEA Software Institute, Madrid, Spain), Pierre-Alain Fouque (Rennes University, CNRS, IRISA, Rennes, France), and Yasemin Acar (The George Washington University, Washington D.C., USA, and MPI-SP, Bochum, Germany)</i>	
Annotating, Tracking, and Protecting Cryptographic Secrets with CryptoMPK .....	650
<i>Xuancheng Jin (Shanghai Jiao Tong University), Xuangan Xiao (Shanghai Jiao Tong University), Songlin Jia (Shanghai Jiao Tong University), Wang Gao (Shanghai Jiao Tong University), Hang Zhang (UC Riverside), Dawu Gu (Shanghai Jiao Tong University), Siqi Ma (The University of Queensland), Zhiyun Qian (UC Riverside), and Juanru Li (Shanghai Jiao Tong University)</i>	

## Session 4A: Spectre and Rowhammer

SoK: Practical Foundations for Software Spectre Defenses .....	666
<i>Sunjay Cauligi (UC San Diego; MPI Security &amp; Privacy), Craig Disselkoen (UC San Diego), Daniel Moghimi (UC San Diego), Gilles Barthe (MPI Security &amp; Privacy; IMDEA Software Institute), and Deian Stefan (UC San Diego)</i>	
SpecHammer: Combining Spectre and Rowhammer for New Speculative Attacks .....	681
<i>Youssef Tobah (University of Michigan), Andrew Kwong (University of Michigan), Ingab Kang (University of Michigan), Daniel Genkin (Georgia Tech), and Kang G. Shin (University of Michigan)</i>	
Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution .....	699
<i>Ayush Agarwal (University of Michigan, USA), Sioli O’Connell (University of Adelaide, Australia), Jason Kim (Georgia Institute of Technology, USA), Shaked Yehezkel (Tel Aviv University, Israel), Daniel Genkin (Georgia Institute of Technology, USA), Eyal Ronen (Tel Aviv University, Israel), and Yuval Yarom (University of Adelaide, Australia)</i>	
Blacksmith: Scalable Rowhammering in the Frequency Domain .....	716
<i>Patrick Jattke (ETH Zurich), Victor van der Veen (Qualcomm Technologies Inc.), Pietro Frigo (VU Amsterdam), Stijn Gunter (ETH Zurich), and Kaveh Razavi (ETH Zurich)</i>	



PROTRR: Principled yet Optimal In-DRAM Target Row Refresh .....	735
<i>Michele Marazzi (ETH Zurich), Patrick Jattke (ETH Zurich), Flavien Solt (ETH Zurich), and Kaveh Razavi (ETH Zurich)</i>	

## Session 4B: Applications of Machine Learning

Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions .....	754
<i>Hammond Pearce (New York University), Baleegh Ahmad (New York University), Benjamin Tan (University of Calgary), Brendan Dolan-Gavitt (New York University), and Ramesh Karri (New York University)</i>	
Spinning Language Models: Risks of Propaganda-as-a-Service and Countermeasures .....	769
<i>Eugene Bagdasaryan (Cornell Tech) and Vitaly Shmatikov (Cornell Tech)</i>	
SoK: How Robust is Image Classification Deep Neural Network Watermarking? .....	787
<i>Nils Lukas (University of Waterloo), Edward Jiang (University of Waterloo), Xinda Li (University of Waterloo), and Florian Kerschbaum (University of Waterloo)</i>	
Transcending TRANSCEND: Revisiting Malware Classification in the Presence of Concept Drift. ....	805
<i>Federico Barbero (King's College London &amp; University of Cambridge, UK), Feargus Pendlebury (Royal Holloway, University of London &amp; The Alan Turing Institute &amp; University College London, UK), Fabio Pierazzi (King's College London, UK), and Lorenzo Cavallaro (University College London, UK)</i>	
Copy, Right? A Testing Framework for Copyright Protection of Deep Learning Models .....	824
<i>Jialuo Chen (Zhejiang University), Jingyi Wang (Zhejiang University), Tinglan Peng (Zhejiang University), Youcheng Sun (University of Manchester, UK), Peng Cheng (Zhejiang University), Shouling Ji (Zhejiang University), Xingjun Ma (Deakin University), Bo Li (University of Illinois Urbana-Champaign), and Dawn Song (University of California, Berkeley)</i>	

## Session 5A: Usability Aspects I

Phishing in Organizations: Findings from a Large-Scale and Long-Term Study .....	842
<i>Daniele Lain (ETH Zurich), Kari Kostianen (ETH Zurich), and Srdjan Capkun (ETH Zurich)</i>	
27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University .....	860
<i>Christian Stransky (Leibniz University Hannover, Germany), Oliver Wiese (Freie Universität Berlin, Germany), Volker Roth (Freie Universität Berlin, Germany), Yasemin Acar (Max Planck Institute for Security and Privacy, Germany), and Sascha Fahl (CISPA / Leibniz University Hannover, Germany)</i>	
Investigating Influencer VPN Ads on YouTube .....	876
<i>Omer Akgul (University of Maryland), Richard Roberts (University of Maryland), Moses Namara (Clemson University), Dave Levin (University of Maryland), and Michelle L. Mazurek (University of Maryland)</i>	

How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study .....	893
<i>Marco Gutfleisch (Ruhr University Bochum, Germany), Jan H. Klemmer (Leibniz University Hannover, Germany), Niklas Busch (Leibniz University Hannover, Germany), Yasemin Acar (Max Planck Institute for Security and Privacy, Germany), M. Angela Sasse (Ruhr University Bochum, Germany), and Sascha Fahl (CISPA / Leibniz University Hannover, Germany)</i>	

## Session 5B: Privacy Applications I

Private Approximate Nearest Neighbor Search with Sublinear Communication .....	911
<i>Sacha Servan-Schreiber (MIT), Simon Langowski (MIT), and Srinivas Devadas (MIT)</i>	
Spiral: Fast, High-Rate Single-Server PIR via FHE Composition .....	930
<i>Samir Jordan Menon (Unaffiliated) and David J. Wu (UT Austin)</i>	
SNARKBlock: Federated Anonymous Blocklisting from Hidden Common Input Aggregate Proofs ...	948
<i>Michael Rosenberg (University of Maryland, College Park), Mary Maller (Ethereum Foundation), and Ian Miers (University of Maryland, College Park)</i>	
How to Attack and Generate Honeywords .....	966
<i>Ding Wang (Nankai University), Yunkai Zou (Nankai University), Qiyong Dong (Nankai University), Yuanming Song (Peking University), and Xinyi Huang (Fujian Normal University)</i>	

## Session 5C: Authentication and Fingerprinting

WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens .....	984
<i>Yan Jiang (Zhejiang University, China), Xiaoyu Ji (Zhejiang University, China), Kai Wang (Zhejiang University, China), Chen Yan (Zhejiang University, China), Richard Mitev (Technical University of Darmstadt, Germany), Ahmad-Reza Sadeghi (Technical University of Darmstadt, Germany), and Wenyuan Xu (Zhejiang University, China)</i>	
Time-Print: Authenticating USB Flash Drives with Novel Timing Fingerprints .....	1002
<i>Patrick Cronin (University of Delaware), Xing Gao (University of Delaware), Haining Wang (Virginia Tech), and Chase Cotton (University of Delaware)</i>	
Device Fingerprinting with Peripheral Timestamps .....	1018
<i>John Monaco (Naval Postgraduate School, USA)</i>	
PCR-Auth: Solving Authentication Puzzle Challenge with Encoded Palm Contact Response ....	1034
<i>Long Huang (Louisiana State University, USA) and Chen Wang (Louisiana State University, USA)</i>	

## Session 6A: Software Security I

Mitigating Information Leakage Vulnerabilities with Type-based Data Isolation .....	1049
<i>Alyssa Milburn (Vrije Universiteit Amsterdam, The Netherlands), Erik van der Kouwe (Vrije Universiteit Amsterdam, The Netherlands), and Cristiano Giuffrida (Vrije Universiteit Amsterdam, The Netherlands)</i>	
SYMBEXCEL: Automated Analysis and Understanding of Malicious Excel 4.0 Macros .....	1066
<i>Nicola Ruaro (University of California, Santa Barbara), Fabio Pagani (University of California, Santa Barbara), Stefano Ortolani (VMware), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)</i>	
HEAPSTER: Analyzing the Security of Dynamic Allocators for Monolithic Firmware Images .....	1082
<i>Fabio Gritti (University of California, Santa Barbara), Fabio Pagani (University of California, Santa Barbara), Ilya Grishchenko (University of California, Santa Barbara), Lukas Dresel (University of California, Santa Barbara), Nilo Redini (Qualcomm Technologies Inc.), Christopher Kruegel (University of California, Santa Barbara), and Giovanni Vigna (University of California, Santa Barbara)</i>	
SoK: Demystifying Binary Lifters Through the Lens of Downstream Applications .....	1100
<i>Zhibo Liu (The Hong Kong University of Science and Technology), Yuanyuan Yuan (The Hong Kong University of Science and Technology), Shuai Wang (The Hong Kong University of Science and Technology), and Yuyan Bao (University of Waterloo)</i>	

## Session 6B: Poisoning and Model Stealing Attacks

Property Inference from Poisoning .....	1120
<i>Saeed Mahloujifar (Princeton), Esha Ghosh (Microsoft Research), and Melissa Chase (Microsoft Research)</i>	
Reconstructing Training Data with Informed Adversaries .....	1138
<i>Borja Balle (DeepMind), Giovanni Cherubin (Microsoft Research), and Jamie Hayes (DeepMind)</i>	
DeepSteal: Advanced Model Extractions Leveraging Efficient Weight Stealing in Memories ....	1157
<i>Adnan Siraj Rakin (Arizona State University), Md Hafizul Islam Chowdhuryy (University of Central Florida), Fan Yao (University of Central Florida), and Deliang Fan (Arizona State University)</i>	
Model Stealing Attacks Against Inductive Graph Neural Networks .....	1175
<i>Yun Shen (Norton Research Group), Xinlei He (CISPA Helmholtz Center for Information Security), Yufei Han (INRIA), and Yang Zhang (CISPA Helmholtz Center for Information Security)</i>	

## Session 6C: Wireless Security

Noise-SDR: Arbitrary Modulation of Electromagnetic Noise from Unprivileged Software and Its Impact on Emission Security .....	1193
<i>Giovanni Camurati (EURECOM, France) and Aurélien Francillon (EURECOM, France)</i>	

mmSpy: Spying Phone Calls using mmWave Radars .....	1211
<i>Suryoday Basak (The Pennsylvania State University) and Mahanth Gowda (The Pennsylvania State University)</i>	
Attacks on Wireless Coexistence: Exploiting Cross-Technology Performance Features for Inter-Chip Privilege Escalation .....	1229
<i>Jiska Classen (Technical University of Darmstadt, Germany), Francesco Gringoli (University of Brescia, Italy), Michael Hermann (Technical University of Darmstadt, Germany), and Matthias Hollick (Technical University of Darmstadt, Germany)</i>	
Invisible Finger: Practical Electromagnetic Interference Attack on Touchscreen-based Electronic Devices .....	1246
<i>Haoqi Shan (University of Florida), Boyi Zhang (University of Florida), Zihao Zhan (University of Florida), Dean Sullivan (University of New Hampshire), Shuo Wang (University of Florida), and Yier Jin (University of Florida)</i>	

## Session 7C: Blockchain Security II

Using Throughput-Centric Byzantine Broadcast to Tolerate Malicious Majority in Blockchains .....	1263
<i>Ruomu Hou (National University of Singapore), Haifeng Yu (National University of Singapore), and Prateek Saxena (National University of Singapore)</i>	
MatRiCT+: More Efficient Post-Quantum Private Blockchain Payments .....	1281
<i>Muhammed F. Esgin (Monash University and CSIRO's Data61, Australia), Ron Steinfeld (Monash University, Australia), and Raymond K. Zhao (Monash University, Australia)</i>	
Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains .....	1299
<i>Sri AravindaKrishnan Thyagarajan (Carnegie Mellon University), Giulio Malavolta (Max Planck Institute for Security and Privacy), and Pedro Moreno-Sanchez (IMDEA Software Institute)</i>	
Foundations of Dynamic BFT .....	1317
<i>Sisi Duan (Tsinghua University) and Haibin Zhang (Beijing Institute of Technology)</i>	
COBRA: Dynamic Proactive Secret Sharing for Confidential BFT Services .....	1335
<i>Robin Vassantlal (LASIGE, Faculdade de Ciencias, Universidade de Lisboa, Portugal), Eduardo Alchieri (Universidade de Brasilia, Brazil), Bernardo Ferreira (LASIGE, Faculdade de Ciencias, Universidade de Lisboa, Portugal), and Alysson Bessani (LASIGE, Faculdade de Ciencias, Universidade de Lisboa, Portugal)</i>	

## Session 7B: Machine Learning Attacks I

Back to the Drawing Board: A Critical Evaluation of Poisoning Attacks on Production Federated Learning .....	1354
<i>Virat Shejwalkar (University of Massachusetts Amherst, USA), Amir Houmansadr (University of Massachusetts Amherst, USA), Peter Kairouz (Google Research, USA), and Daniel Ramage (Google Research, USA)</i>	

Model Orthogonalization: Class Distance Hardening in Neural Networks for Better Security .	1372
<i>Guanhong Tao (Purdue University), Yingqi Liu (Purdue University), Guangyu Shen (Purdue University), Qiuling Xu (Purdue University), Shengwei An (Purdue University), Zhuo Zhang (Purdue University), and Xiangyu Zhang (Purdue University)</i>	
Universal 3-Dimensional Perturbations for Black-Box Attacks on Video Recognition Systems	1390
<i>Shangyu Xie (Illinois Institute of Technology, USA), Han Wang (Illinois Institute of Technology, USA), Yu Kong (Rochester Institute of Technology, USA), and Yuan Hong (Illinois Institute of Technology, USA)</i>	
"Adversarial Examples" for Proof-of-Learning .....	1408
<i>Rui Zhang (Zhejiang University, China), Jian Liu (Zhejiang University, China), Yuan Ding (Zhejiang University, China), Zhibo Wang (Zhejiang University, China), Qingbiao Wu (Zhejiang University, China), and Kui Ren (Zhejiang University, China)</i>	
Transfer Attacks Revisited: A Large-Scale Empirical Study in Real Computer Vision Settings....	1423
<i>Yuhao Mao (Zhejiang University, China), Chong Fu (Zhejiang Univeristy, China), Saizhuo Wang (Zhejiang Univeristy, China), Shouling Ji (Zhejiang University, China), Xuhong Zhang (Zhejiang University, China), Zhenguang Liu (Zhejiang Gongshang University, China), Jun Zhou (Ant Group, China), Alex Liu (Ant Group, China), Raheem Beyah (Georgia Institute of Technology, the United States), and Ting Wang (Pennsylvania State University, the United States)</i>	

## Session 7A: Side-Channel Attacks

Graphics Peeping Unit: Exploiting EM Side-Channel Information of GPUs to Eavesdrop on Your Neighbors .....	1440
<i>Zihao Zhan (Vanderbilt University, USA; University of Florida, USA), Zhenkai Zhang (Clemson University, USA), Sisheng Liang (Clemson University, USA), Fan Yao (University of Central Florida, USA), and Xenofon Koutsoukos (Vanderbilt University, USA)</i>	
Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks .....	1458
<i>Yanan Guo (University of Pittsburgh), Andrew Zigerelli (Independent Researcher), Youtao Zhang (University of Pittsburgh), and Jun Yang (University of Pittsburgh)</i>	
Finding and Exploiting CPU Features using MSR Templating .....	1474
<i>Andreas Kogler (Graz University of Technology), Daniel Weber (CISPA Helmholtz Center for Information Security), Martin Haubenwallner (Graz University of Technology), Moritz Lipp (Amazon Web Services), Daniel Gruss (Graz University of Technology), and Michael Schwarz (CISPA Helmholtz Center for Information Security)</i>	
Augury: Using data memory-dependent prefetchers to leak data at rest .....	1491
<i>Jose Sanchez Vicarte (University of Illinois at Urbana-Champaign), Michael Flanders (University of Washington), Riccardo Paccagnella (University of Illinois at Urbana-Champaign), Grant Garrett-Grossman (University of Illinois at Urbana-Champaign), Adam Morrison (Tel Aviv University), Chris Fletcher (University of Illinois at Urbana-Champaign), and David Kohlbrenner (University of Washington)</i>	

MeshUp: Stateless Cache Side-channel Attack on CPU Mesh .....	1506
<i>Junpeng Wan (Fudan University), Yanxiang Bi (Fudan University), Zhe Zhou (Fudan University), and Zhou Li (University of California, Irvine)</i>	

## Session 8A: Web Security

Timing-Based Browsing Privacy Vulnerabilities via Site Isolation .....	1525
<i>Zihao Jin (Microsoft Research Asia and Tsinghua University, China), Ziqiao Kong (Microsoft Research Asia, China), Shuo Chen (Microsoft Research Asia), and Haixin Duan (Tsinghua University, China)</i>	
WtaGraph: Web Tracking and Advertising Detection using Graph Neural Networks .....	1540
<i>Zhiju Yang (Colorado School of Mines), Weiping Pei (Colorado School of Mines), Monchu Chen (Appen), and Chuan Yue (Colorado School of Mines)</i>	
Surakav: Generating Realistic Traces for a Strong Website Fingerprinting Defense .....	1558
<i>Jiajun Gong (The Hong Kong University of Science and Technology), Wuqi Zhang (The Hong Kong University of Science and Technology), Charles Zhang (The Hong Kong University of Science and Technology), and Tao Wang (Simon Fraser University)</i>	
Wobfuscator: Obfuscating JavaScript Malware via Opportunistic Translation to WebAssembly .....	1574
<i>Alan Romano (University at Buffalo, SUNY), Daniel Lehmann (University of Stuttgart), Michael Pradel (University of Stuttgart), and Weihang Wang (University at Buffalo, SUNY)</i>	
The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies .....	1590
<i>Soheil Khodayari (CISPA Helmholtz Center for Information Security, Germany) and Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security, Germany)</i>	

## Session 8B: Embedded Security

IRQDebloat: Reducing Driver Attack Surface in Embedded Devices .....	1608
<i>Zhenghao Hu (New York University) and Brendan Dolan-Gavitt (New York University)</i>	

Finding SMM Privilege-Escalation Vulnerabilities in UEFI Firmware with Protocol-Centric Static Analysis .....	1623
<i>Jiawei Yin (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Menghao Li (Beijing Key Laboratory of Network Security and Protection Technology), Wei Wu (Huawei Technology), Dandan Sun (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Jianhua Zhou (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), Wei Huo (Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology), and Jingling Xue (UNSW Sydney)</i>	
Mind the Gap: Studying the Insecurity of Provably Secure Embedded Trusted Execution Architectures .....	1638
<i>Marton Bognar (imec-DistriNet, KU Leuven), Jo Van Bulck (imec-DistriNet, KU Leuven), and Frank Piessens (imec-DistriNet, KU Leuven)</i>	
How Not to Protect Your IP - An Industry-Wide Break of IEEE 1735 Implementations .....	1656
<i>Julian Speith (Max Planck Institute for Security and Privacy, Germany &amp; Ruhr University Bochum, Germany), Florian Schweins (Ruhr University Bochum, Germany), Maik Ender (Max Planck Institute for Security and Privacy, Germany &amp; Ruhr University Bochum, Germany), Marc Fyrbiak (Max Planck Institute for Security and Privacy, Germany), Alexander May (Ruhr University Bochum, Germany), and Christof Paar (Max Planck Institute for Security and Privacy, Germany &amp; Ruhr University Bochum, Germany)</i>	
Hardening Circuit-Design IP Against Reverse-Engineering Attacks .....	1672
<i>Animesh Chhotaray (University of Florida, USA) and Thomas Shrimpton (University of Florida, USA)</i>	

## Session 8C: Physical Layer Security

Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices .....	1690
<i>Hadi Givchian (UC San Diego), Nishant Bhaskar (UC San Diego), Eliana Rodriguez Herrera (UC San Diego), Hector Lopez Soto (UC San Diego), Christian Dameff (UC San Diego), Dinesh Bharadia (UC San Diego), and Aaron Schulman (UC San Diego)</i>	

IRShield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing .....	1705
<i>Paul Staat (Max Planck Institute for Security and Privacy), Simon Mulzer (Ruhr University Bochum), Stefan Roth (Ruhr University Bochum), Veelasha Moonsamy (Ruhr University Bochum), Markus Heinrichs (TH Köln – University of Applied Sciences), Rainer Kronberger (TH Köln – University of Applied Sciences), Aydin Sezgin (Ruhr University Bochum), and Christof Paar (Max Planck Institute for Security and Privacy)</i>	
Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems .....	1722
<i>Paul Staat (Max Planck Institute for Security and Privacy), Johannes Tobisch (Max Planck Institute for Security and Privacy), Christian Zenger (Physec GmbH), and Christof Paar (Max Planck Institute for Security and Privacy)</i>	
Practical EMV Relay Protection .....	1737
<i>Andreea-Ina Radu (University of Birmingham, UK), Tom Chothia (University of Birmingham, UK), Christopher J.P. Newton (University of Surrey, UK), Ioana Boureanu (University of Surrey, UK), and Liqun Chen (University of Surrey, UK)</i>	
AccEar: Accelerometer Acoustic Eavesdropping with Unconstrained Vocabulary .....	1757
<i>Pengfei Hu (Shandong University), Hui Zhuang (Shandong University), Panneer Selvam Santhalingam (George Mason University), Riccardo Spolaor (Shandong University), Parth Pathak (George Mason University), Guoming Zhang (Shandong University), and Xiuzhen Cheng (Shandong University)</i>	

## Session 9A: Auditing and Vulnerability Analysis

Towards Automated Auditing for Account and Session Management Flaws in Single Sign-On Deployments .....	1774
<i>Mohammad Ghasemisharif (University of Illinois at Chicago), Chris Kanich (University of Illinois at Chicago), and Jason Polakis (University of Illinois at Chicago)</i>	
HardLog: Practical Tamper-Proof System Auditing Using a Novel Audit Device .....	1791
<i>Adil Ahmad (Purdue), Sangho Lee (Microsoft Research), and Marcus Peinado (Microsoft Research)</i>	
SwarmFlawFinder: Discovering and Exploiting Logic Flaws of Swarm Algorithms .....	1808
<i>Chijung Jung (University of Virginia), Ali Ahad (University of Virginia), Yuseok Jeon (Ulsan National Institute of Science and Technology), and Yonghwi Kwon (University of Virginia)</i>	
PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles .....	1826
<i>Hyungsub Kim (Purdue University), Muslum Ozgur Ozmen (Purdue University), Z. Berkay Celik (Purdue University), Antonio Bianchi (Purdue University), and Dongyan Xu (Purdue University)</i>	



## Session 9B: Usability Aspects II and ML Attacks

“Flawed, but like democracy we don’t have a better system”: The Experts’ Insights on the Peer Review Process of Evaluating Security Papers .....	1845
<i>Ananta Soneji (Arizona State University, USA), Faris Bugra Kokulu (Arizona State University, USA), Carlos Rubio-Medrano (Texas A&amp;M University - Corpus Christi, USA), Tiffany Bao (Arizona State University, USA), Ruoyu Wang (Arizona State University, USA), Yan Shoshitaishvili (Arizona State University, USA), and Adam Doupé (Arizona State University, USA)</i>	
SoK: Social Cybersecurity .....	1863
<i>Yuxi Wu (Georgia Institute of Technology), W. Keith Edwards (Georgia Institute of Technology), and Sauvik Das (Georgia Institute of Technology)</i>	
Committed to Trust: A Qualitative Study on Security & Trust in Open Source Software Projects .....	1880
<i>Dominik Wermke (CISPA Helmholtz Center for Information Security, Germany), Noah Woehler (CISPA Helmholtz Center for Information Security, Germany), Jan H. Klemmer (Leibniz University Hannover, Germany), Marcel Fourné (Max Planck Institute for Security and Privacy, Germany), Yasemin Acar (George Washington University, USA), and Sascha Fahl (CISPA Helmholtz Center for Information Security and Leibniz University Hannover, Germany)</i>	
Membership Inference Attacks from First Principles .....	1897
<i>Nicholas Carlini (Google Research), Steve Chien (Google Research), Milad Nasr (Google Research, University of Massachusetts Amherst), Shuang Song (Google Research), Andreas Terzis (Google Research), and Florian Tramer (Google Research)</i>	

## Session 9C: Privacy

DeepCoFFEA: Improved Flow Correlation Attacks on Tor via Metric Learning and Amplification.....	1915
<i>Se Eun Oh (Ewha Womans University), Taiji Yang (University of Minnesota), Nate Mathews (Rochester Institute of Technology), James Holland (University of Minnesota), Mohammad Saidur Rahman (Rochester Institute of Technology), Nicholas Hopper (University of Minnesota), and Matthew Wright (Rochester Institute of Technology)</i>	
ShorTor: Improving Tor Network Latency via Multi-hop Overlay Routing .....	1933
<i>Kyle Hogan (Massachusetts Institute of Technology, United States), Sacha Servan-Schreiber (Massachusetts Institute of Technology, United States), Zachary Newman (Massachusetts Institute of Technology, United States), Ben Weintraub (Northeastern University, United States), Cristina Nita-Rotaru (Northeastern University, United States), and Srinivas Devadas (Massachusetts Institute of Technology, United States)</i>	
Sabre: Sender-Anonymous Messaging with Fast Audits .....	1953
<i>Adithya Vadapalli (University of Waterloo, Canada), Kyle Storrier (University of Calgary, Canada), and Ryan Henry (University of Calgary, Canada)</i>	

Security Foundations for Application-Based Covert Communication Channels .....	1971
<i>James K. Howes (University of Florida), Marios Georgiou (Galois, Inc.), Alex J. Malozemoff (Galois, Inc.), and Thomas Shrimpton (University of Florida)</i>	

## Session 10B: Machine Learning Attacks II

Bad Characters: Imperceptible NLP Attacks .....	1987
<i>Nicholas Boucher (University of Cambridge, United Kingdom), Iliia Shumailov (University of Cambridge and Vector Institute, United Kingdom), Ross Anderson (University of Cambridge and University of Edinburgh, United Kingdom), and Nicolas Papernot (University of Toronto and Vector Institute, Canada)</i>	
LinkTeller: Recovering Private Edges from Graph Neural Networks via Influence Analysis .....	2005
<i>Fan Wu (University of Illinois at Urbana-Champaign, USA), Yunhui Long (University of Illinois at Urbana-Champaign, USA), Ce Zhang (ETH Zurich, Switzerland), and Bo Li (University of Illinois at Urbana-Champaign, USA)</i>	
PICCOLO: Exposing Complex Backdoors in NLP Transformer Models .....	2025
<i>Yingqi Liu (Purdue University, US), Guangyu Shen (Purdue University, US), Guanhong Tao (Purdue University, US), Shengwei An (Purdue University, US), Shiqing Ma (Rutgers University, US), and Xiangyu Zhang (Purdue University, US)</i>	
BadEncoder: Backdoor Attacks to Pre-trained Encoders in Self-Supervised Learning .....	2043
<i>Jinyuan Jia (Duke University, USA), Yupei Liu (Duke University, USA), and Neil Zhenqiang Gong (Duke University, USA)</i>	

## Session 10C: Software Security II

Repairing DoS Vulnerability of Real-World Regexes .....	2060
<i>Nariyoshi Chida (NTT Corporation / Waseda University, Japan) and Tachio Terauchi (Waseda University, Japan)</i>	
GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs .....	2078
<i>Zhenpeng Lin (The Pennsylvania State University), Yueqi Chen (The Pennsylvania State University), Yuhang Wu (The Pennsylvania State University), Chensheng Yu (George Washington University), Dongliang Mu (School of Cyber Science and Engineering, HUST), Xinyu Xing (Northwestern University), and Kang Li (Baidu USA)</i>	
Goshawk: Hunting Memory Corruptions via Structure-Aware and Object-Centric Memory Operation Synopsis .....	2096
<i>Yunlong Lyu (University of Science and Technology of China, China), Yi Fang (Feiyu Security, China), Yiwei Zhang (Shanghai Jiao Tong University, China), Qibin Sun (University of Science and Technology of China, China), Siqi Ma (The University of New South Wales, Australia), Elisa Bertino (Purdue University, USA), Kangjie Lu (University of Minnesota, USA), and Juanru Li (Shanghai Jiao Tong University, China)</i>	

FSAFlow: Lightweight and Fast Dynamic Path Tracking and Control for Privacy Protection on Android Using Hybrid Analysis with State-Reduction Strategy .....	2114
<i>Zhi Yang (PLA Information Engineering University, China), Zhanhui Yuan (PLA Information Engineering University, China), Shuyuan Jin (SUN Yat-Sen University, China), Xingyuan Chen (PLA Information Engineering University, China), Lei Sun (PLA Information Engineering University, China), Xuehui Du (PLA Information Engineering University,, China), Wenfa Li (University of Science and Technology Beijing, China), and Hongqi Zhang (PLA Information Engineering University, China)</i>	

## Session 10A: Measurement Studies I

Domains Do Change Their Spots: Quantifying Potential Abuse of Residual Trust .....	2130
<i>Johnny So (Stony Brook University, USA), Najmeh Miramirkhani (Stony Brook University, USA), Michael Ferdman (Stony Brook University, USA), and Nick Nikiforakis (Stony Brook University, USA)</i>	
Scraping Sticky Leftovers: App User Information Left on Servers After Account Deletion .....	2145
<i>Preethi Santhanam (Wichita State University), Hoang Dang (Wichita State University), Zhiyong Shan (Wichita State University), and Iulian Neamtiu (New Jersey Institute of Technology)</i>	
TROLLMAGNIFIER: Detecting State-Sponsored Troll Accounts on Reddit .....	2161
<i>Mohammad Hammas Saeed (Boston University), Shiza Ali (Boston University), Jeremy Blackburn (Binghamton University), Emiliano De Cristofaro (University College London), Savvas Zannettou (TU Delft, Max Planck Institute for Informatics), and Gianluca Stringhini (Boston University)</i>	
Analyzing Ground-Truth Data of Mobile Gambling Scams .....	2176
<i>Geng Hong (Fudan University, China), Zhemin Yang (Fudan University, China), Sen Yang (Fudan University, China), Xiaojing Liao (Indiana University Bloomington, USA), Xiaolin Du (Fudan University, China), Min Yang (Fudan University, China), and Haixin Duan (Tsinghua University, China; Qi An Xin Group Corp., China)</i>	

## Session 11A: Fuzzing II

Effective Seed Scheduling for Fuzzing with Graph Centrality Analysis .....	2194
<i>Dongdong She (Columbia University), Abhishek Shah (Columbia University), and Suman Jana (Columbia University)</i>	
FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks .....	2212
<i>Kyungtae Kim (Purdue University, USA), Taegy Kim (Pennsylvania State University, USA), Ertza Warraich (Purdue University, USA), Byoungyoung Lee (Seoul National University, South Korea), Kevin Butler (University of Florida, USA), Antonio Bianchi (Purdue University, USA), and Dave Tian (Purdue University, USA)</i>	

Exploit the Last Straw That Breaks Android Systems .....	2230
<i>Lei Zhang (Fudan University, China), Keke Lian (Fudan University, China), Haoyu Xiao (Fudan University, China), Zhibo Zhang (Fudan University, China), Peng Liu (The Pennsylvania State University, United States of America), Yuan Zhang (Fudan University, China), Min Yang (Fudan University, China), and Haixin Duan (Tsinghua University, China)</i>	

## Session 11B: Formal Method Applications

CirC: Compiler Infrastructure for Proof Systems, Software Verification, and More .....	2248
<i>Alex Ozdemir (Stanford University), Fraser Brown (Stanford University and Carnegie Mellon University), and Riad Wahby (Stanford University and Carnegie Mellon University)</i>	
HAMRAZ: Resilient Partitioning and Replication .....	2267
<i>Xiao Li (University of California, Riverside, USA), Farzin Houshmand (University of California, Riverside, USA), and Mohsen Lesani (University of California, Riverside, USA)</i>	
Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities .....	2285
<i>Jianliang Wu (Purdue University), Ruoyu Wu (Purdue University), Dongyan Xu (Purdue University), Dave Tian (Purdue University), and Antonio Bianchi (Purdue University)</i>	

## Session 11C: Usable Security

“Desperate Times Call for Desperate Measures”: User Concerns with Mobile Loan Apps in Kenya .....	2304
<i>Collins W. Munyendo (The George Washington University), Yasemin Acar (The George Washington University), and Adam J. Aviv (The George Washington University)</i>	
SoK: The Dual Nature of Technology in Sexual Abuse .....	2320
<i>Borke Obada-Obieh (University of British Columbia), Yue Huang (University of British Columbia), Lucrezia Spagnolo (Vesta Social Innovation Technologies), and Konstantin Beznosov (University of British Columbia)</i>	
SoK: A Framework for Unifying At-Risk User Research .....	2344
<i>Noel Warford (University of Maryland College Park), Tara Matthews (Google), Kaitlyn Yang (University of Maryland College Park), Omer Akgul (University of Maryland College Park), Sunny Consolvo (Google), Patrick Gage Kelley (Google), Nathan Malkin (University of Maryland College Park), Michelle L. Mazurek (University of Maryland College Park), Manya Sleeper (Google), and Kurt Thomas (Google)</i>	

## Session 12A: Measurement Studies II and IoT Security

Deployment of Source Address Validation by Network Operators: A Randomized Control Trial .....	2361
<i>Qasim Lone (Delft University of Technology), Alisa Frik (ICSI, UC Berkeley), Matthew Luckie (University of Waikato), Maciej Korczynski (Grenoble INP), Michel van Eeten (Delft University of Technology), and Carlos Gañán (Delft University of Technology)</i>	
Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices .....	2379
<i>Takayuki Sasaki (Yokohama National University), Akira Fujita (Yokohama National University/National Institute of Information and Communications Technology), Carlos Ganan (TU Delft/Yokohama National University), Michel van Eeten (TU Delft/Yokohama National University), Katsunari Yoshioka (Yokohama National University), and Tsutomu Matsumoto (Yokohama National University)</i>	
Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms .....	2397
<i>Zhi Li (School of Cyber Science and Engineering, Huazhong University of Science and Technology, China; School of Computer Science and Technology, Huazhong University of Science and Technology, China; National Engineering Research Center for Big Data Technology and System, China; Cluster and Grid Computing Lab, China; Services Computing Technology and System Lab, China; Big Data Security Engineering Research Center, China), Weijie Liu (Indiana University Bloomington, USA), Hongbo Chen (Indiana University Bloomington, USA), XiaoFeng Wang (Indiana University Bloomington, USA), Xiaojing Liao (Indiana University Bloomington, USA), Luyi Xing (Indiana University Bloomington, USA), Mingming Zha (Indiana University Bloomington, USA), Hai Jin (School of Computer Science and Technology, Huazhong University of Science and Technology, China; National Engineering Research Center for Big Data Technology and System, China; Cluster and Grid Computing Lab, China; Services Computing Technology and System Lab, China; Big Data Security Engineering Research Center, China), and Deqing Zou (School of Cyber Science and Engineering, Huazhong University of Science and Technology, China; National Engineering Research Center for Big Data Technology and System, China; Cluster and Grid Computing Lab, China; Services Computing Technology and System Lab, China; Big Data Security Engineering Research Center, China)</i>	
Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors with VERSA .....	2413
<i>Ivan De Oliveira Nunes (Rochester Institute of Technology), Seoyeon Hwang (University of California Irvine), Sashidhar Jakkamsetti (University of California Irvine), and Gene Tsudik (University of California Irvine)</i>	

## Session 12B: Privacy Applications II

Publicly Accountable Robust Multi-party Computation .....	2430
<i>Marc Rivinius (University of Stuttgart, Germany), Pascal Reisert (University of Stuttgart, Germany), Daniel Rausch (University of Stuttgart, Germany), and Ralf Küsters (University of Stuttgart, Germany)</i>	
Waldo: A Private Time-Series Database from Function Secret Sharing .....	2450
<i>Emma Dauterman (UC Berkeley), Mayank Rathee (UC Berkeley), Raluca Ada Popa (UC Berkeley), and Ion Stoica (UC Berkeley)</i>	
Hark: A Deep Learning System for Navigating Privacy Feedback at Scale .....	2469
<i>Hamza Harkous (Google), Sai Teja Peddinti (Google), Rishabh Khandelwal (University of Wisconsin - Madison), Animesh Srivastava (Google), and Nina Taft (Google)</i>	
Sphinx: Enabling Privacy-Preserving Online Learning over the Cloud .....	2487
<i>Han Tian (Hong Kong University of Science and Technology), Chaoliang Zeng (Hong Kong University of Science and Technology), Zhenghang Ren (Hong Kong University of Science and Technology), Di Chai (Hong Kong University of Science and Technology; Clustar), Juexue Zhang (Hong Kong University of Science and Technology; Clustar), Kai Chen (Hong Kong University of Science and Technology), and Qiang Yang (Hong Kong University of Science and Technology)</i>	

## Session 12C: Key Distribution

SPURT: Scalable Distributed Randomness Beacon with Transparent Setup .....	2502
<i>Sourav Das (University of Illinois at Urbana-Champaign), Vinith Krishnan (University of Illinois at Urbana-Champaign), Irene Miriam Isaac (University of Illinois at Urbana-Champaign), and Ling Ren (University of Illinois at Urbana-Champaign)</i>	
Practical Asynchronous Distributed Key Generation .....	2518
<i>Sourav Das (University of Illinois at Urbana-Champaign), Thomas Yurek (University of Illinois at Urbana-Champaign), Zhuolun Xiang (University of Illinois at Urbana-Champaign), Andrew Miller (University of Illinois at Urbana-Champaign), Lefteris Kokoris-Kogias (IST Austria), and Ling Ren (University of Illinois at Urbana-Champaign)</i>	
Security Analysis of the MLS Key Derivation .....	2535
<i>Chris Brzuska (Aalto University, Finland), Eric Cornelissen (Aalto University, Finland), and Konrad Kohbrok (Aalto University, Finland)</i>	
Low-Bandwidth Threshold ECDSA via Pseudorandom Correlation Generators .....	2554
<i>Damiano Abram (Aarhus University), Ariel Nof (Technion), Claudio Orlandi (Aarhus University), Peter Scholl (Aarhus University), and Omer Shlomovits (ZenGo X)</i>	

## Author Index